disseminate IIF, according to DON PIA guidance found at *http://www.privacy.navy.mil* and *http://www.doncio.navy.mil*.

(8) Complete and maintain a disclosure accounting form for all disclosures made without the consent of the record subject, except those made within DOD or under FOIA. (See 701.111).

(9) Ensure that only those DOD/DON officials with a ''need to know'' in the official performance of their duties has access to information contained in a system of records.

(10) Ensure safeguards are in place to protect the privacy of individuals and confidentiality of PPI contained in a system of records.

(11) Ensure that records are maintained in accordance with the identified PA systems of records notice.

(12) Ensure that each newly proposed PA system of records notice is evaluated for need and relevancy and confirm that no existing PA system of records notice covers the proposed collection.

(13) Stop collecting any category or item of information about individuals that is no longer justified, and when feasible remove the information from existing records.

(14) Ensure that records are kept in accordance with retention and disposal requirements set forth in SECNAVINST 5720.47B.

(15) Take reasonable steps to ensure the accuracy, relevancy, timeliness, and completeness of a record before disclosing the record to anyone outside the Federal Government.

(16) Identify all systems of records that are maintained in whole or in part by contractor personnel, ensuring that they are properly trained and that they are routinely inspected for PA compliance.

§ 701.105 Policy.

DON recognizes that the privacy of an individual is a personal and fundamental right that shall be respected and protected and that PPI shall be collected, maintained, used, or disclosed to ensure that it is relevant and necessary to accomplish a lawful DON/DOD purpose required to be accomplished by statute or Executive Order (E.O.). Accordingly, it is DON policy that DON activities shall fully comply with 5 U.S.C. 552a, DOD Directive 5400.11 and DOD 5400.11–R to protect individuals from unwarranted invasions of privacy when information is collected, processed, maintained, or disseminated. To ensure compliance, DON activities shall follow the procedures listed in this section.

(a) *Collection, maintenance and use.* (1) Only maintain systems of records that have been approved and published in the FEDERAL REGISTER. (See *http://www.privacy.navy.mil* for a list of all DOD, Navy, Marine Corps, and component systems of records notices, as well as, links to Government-wide systems that the DON is eligible to use).

NOTE: CNO (DNS–36) can assist Navy activities in identifying existing systems that may meet their needs and HQMC (ARSF) can assist Marine Corps activities.

(2) Only collect, maintain, and use PPI needed to support a DON function or program as authorized by law or E.O. and disclose this information only as authorized by 5 U.S.C. 552a, this subpart and subpart G of this part. In assessing need, DON activities shall consider alternatives such as: truncating the SSN by only using the last four digits; using information that is not individually identifiable; using a sampling of certain data for certain individuals only. Additionally, they shall consider the length of time the information is needed and the cost of maintaining the information compared to the risks and adverse consequences of not maintaining the information.

(3) Only maintain PPI that is timely, accurate, complete, and relevant to the purpose for which it was collected.

(4) DON activities shall not maintain records describing how an individual exercises his/her rights guaranteed by the First Amendment (freedom of religion; freedom of political beliefs; freedom of speech; freedom of the press; the right to peaceful assemblage; and petition for redress of grievances), unless they are: expressly authorized by statute; authorized by the individual; within the scope of an authorized law enforcement activity; or are used for the maintenance of certain items of information relating to religious affiliation for members of the naval service who are chaplains.

NOTE: This should not be construed, however, as restricting or excluding solicitation of information that the individual is willing to have in his/her record concerning religious preference, particularly that required in emergency situations.

(b) *Disposal.* Dispose of records from systems of records to prevent inadvertent disclosure. To this end:

(1) Disposal methods are considered adequate if the records are rendered unrecognizable or beyond reconstruction (e.g., tearing, burning, melting, chemical decomposition, burying, pulping, pulverizing, shredding, or mutilation). Magnetic media may be cleared by completely erasing, overwriting, or degaussing the tape.

(2) DON activities may recycle PA data. Such recycling must be accomplished to ensure that PPI is not compromised. Accordingly, the transfer of large volumes of records in bulk to an authorized disposal activity is not considered a disclosure of records.

(3) When disposing of or destroying large quantities of records from a system of records, DON activities must ensure that the records are disposed of to preclude easy identification of specific records.

(c) *Individual access.* (1) Allow individuals to have access to and/or copies of all or portions of their records to which they are entitled. In the case of a legal guardian or custodial parent of a minor, they have the same rights as the individual he/she represents. A minor is defined as an individual under the age of 18. In the case of members of the Armed Forces under the age of 18, they are not considered to be minors for the purposes of the PA.

(2) Enter all PA first-party access requests into a tracking system and assign a case file number. (Files should comply with DON PA systems of records notice NM05211–1, PA Request Files and Tracking System at *http://www.privacy.navy.mil/notices.*)

(3) Allow individuals to seek amendment of their records when they can identify and provide proof that factual information contained therein is erroneous, untimely, incomplete, or irrelevant. While opinions are not subject to amendment, individuals who are denied access to amending their record may have a statement of disagreement added to the file.

(4) Allow individuals to appeal decisions that deny them access to or refusal to amend their records. If a request to amend their record is denied, allow the individual to file a written statement of disagreement.

(d) *Posting and use of PA sensitive information.* (1) Do not post PPI on an Internet site. Also, limit the posting and use of PA sensitive information on an Intranet Web site, letter, FAX, e-mail, etc.

(2) When posting or transmitting PPI, ensure the following legend is posted on the document: ''FOR OFFICIAL USE ONLY—PRIVACY ACT SENSITIVE: Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties.''

(e) *Safeguarding PPI.* DON activities shall establish appropriate administrative, technical and physical safeguards to ensure that the records in every system of records are protected from unauthorized alteration or disclosure and that their confidentiality is protected. Protect the records against reasonably anticipated threats of hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is kept. At a minimum, DON activities shall:

(1) Tailor system safeguards to conform to the type of records in the system, the sensitivity of the PPI stored, the storage medium used, and the number of records maintained.

(2) Treat all unclassified records that contain PPI that normally would be withheld from the public under FOIA exemptions (b)(6) and (b)(7)(C) as if they were designated ''For Official Use Only'' and safeguard them from unauthorized disclosure.

(3) Ensure that privacy considerations are addressed in the reengineering of business processes and take proactive steps to ensure compliance with the PA and 5 U.S.C. 552a as they move from conducting routine business via paper to electronic media.

(4) Recognize the importance of protecting the privacy of its members, especially as it modernizes its collection systems. Privacy issues must be addressed when systems are being developed, and privacy protections must be

integrated into the development life cycle of automated systems. This applies also to contractors, vendors, and other entities that develop, procure, or use IT systems under contract to DOD/DON, to collect, maintain, or disseminate IIF from or about members of the public (see § 701.115).

(5) Ensure that adequate safeguards are implemented and enforced to prevent misuse, unauthorized disclosure, alteration, or destruction of PPI in records per 5 U.S.C. 552a, this subpart and subpart G of this part.

§ 701.106 Collecting information about individuals.

(a) *Collecting information directly from the individual.* To the greatest extent practicable, collect information for systems of records directly from the individual to whom the record pertains if the record may be used to make an adverse determination about the individual's rights, benefits, or privileges under a Federal program.

(b) *Collecting information about individuals from third persons.* It may not always be practical to collect all information about an individual directly. For example, when verifying information through other sources for security or employment suitability determinations; seeking other opinions, such as a supervisor's comments on past performance or other evaluations; obtaining the necessary information directly from the individual would be exceptionally difficult or would result in unreasonable costs or delays; or, the individual requests or consents to contacting another person to obtain the information.

(c) *Soliciting the SSN.* (1) It is unlawful for any Federal, State, or local government agency to deny an individual a right, benefit, or privilege provided by law because the individual refuses to provide his/her SSN. However, this prohibition does not apply if a Federal law requires that the SSN be provided, or the SSN is required by a law or regulation adopted before January 1, 1975, to verify the individual's identity for a system of records established and in use before that date.

(2) Before requesting an individual to provide the SSN, the individual must be advised whether providing the SSN is mandatory or voluntary; by what law or other authority the SSN is solicited; and what uses will be made of the SSN.

(3) The preceding advice relates only to the SSN. If other information about the individual is solicited for a system of records, a PAS also must be provided.

(4) The notice published in the FEDERAL REGISTER for each system of records containing SSNs solicited from individuals must indicate the authority for soliciting the SSNs and whether it is mandatory for the individuals to provide their SSN. E.O. 9397 requires Federal Agencies to use SSNs as numerical identifiers for individuals in most Federal records systems. However, it does not make it mandatory for individuals to provide their SSNs.

(5) When entering military service or civilian employment with the DON, individuals are asked to provide their SSNs. In many instances, this becomes the individual's numerical identifier and is used to establish personnel, financial, medical, and other official records (as authorized by E.O. 9397). The individuals must be given the notification described above. Once the individual has provided his/her SSN to establish a record, a notification is not required when the SSN is requested only for identification or to locate the records.

(6) DON activities are discouraged from collecting SSNs when another identifier would suffice. In those instances where activities wish to differentiate individuals, they may find it advantageous to only collect the last four digits of the individual's SSN, which is not considered to be privacy sensitive.

(7) If a DON activity requests an individual's SSN even though it is not required by Federal statute, or is not for a system of records in existence and operating prior to January 1, 1975, it must provide a PAS and make it clear that disclosure of the number is voluntary. Should the individual refuse to disclose his/her SSN, the activity must be prepared to identify the individual by alternate means.

(d) *Contents of a PAS.* (1) When an individual is requested to furnish PPI for possible inclusion in a system of